BÁO CÁO THỰC HÀNH

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Lab 02 – Triển khai Snort Inline

GVHD: Đỗ Hoàng Hiển

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Viết Dũng	21520747	21520090@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521112@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1: Sinh viên trả lời các câu hỏi bên dưới

1.1a. Tìm hiểu về Snort? Snort cho phép chạy trên những chế độ (mode) nào?

→ Snort là một NIDPS mã nguồn mở dựa trên kỹ thuật phát hiện Signature-based NIDPS. Sử dụng một tập các bộ rules định nghĩa dấu hiệu của tấn công cho việc nhận diện tấn công. Quản trị viên mạng có thể phát hiện các cuộc tấn công từ chối dịch vụ DoS, tấn công DoS phân tán DDoS, tấn công CGI (Common Gateway Inteface), tràn bộ đệm, scan port,…

* Snort cho phép chạy trên các mode:

- *Sniff mode* (snort -v): thu thập và phân tích gói tin.

- *Packet logger mode* (snort -l /var/log/snort): tập hợp packet nó thấy và đưa vào log

- *NIDS mode* (snort -c /etc/snort/snort.conf -I eth0): Chế độ chính của Snort, phát hiện tấn công/hành vi xâm nhập độc hại.

- *Inline mode*: cho phép phân tích các gói tin từ firewall iptables sử dụng các tập lệnh mới như: pass, drop, reject để ngăn chặn các hoạt động độc hại.

1.1b. Trình bày những tính năng chính của Snort?

→ Tính năng chính của Snort:

- Bắt lưu lượng mạng đang truyền và phân tích lưu lượng mạng theo thời gian thực.
- Phân tích giao thức, tìm kiếm/so khớp nội dung.
- Ghi log các sự kiện, thông tin.
- Nhận diện, phát hiện tấn công hoặc do thám dựa trên các rules và các thông tin phân tích được.

2. Yêu cầu 2: Cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụp lại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm

Mô hình mạng triển khai sẽ là: **10.81.27.0/24** và **192.168.27.0/24**, trong đó 2 là chữ số cuối trong MSSV của Huỳnh Như, và 7 là chữ số cuối trong MSSV của Viết Dũng.

2.1a. Cấu hình mạng cho các máy theo mô hình

- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP:

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Custom	-	-	Enabled	192.168.42.0
VMnet8	NAT	NAT	-	Enabled	192.168.27.0

- Gán các card mạng cho máy Router:

Network Adapter	NAT
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet3)

- Gán các card mạng cho máy Kali:

CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet2)

- Gán các card mạng cho máy Snort:

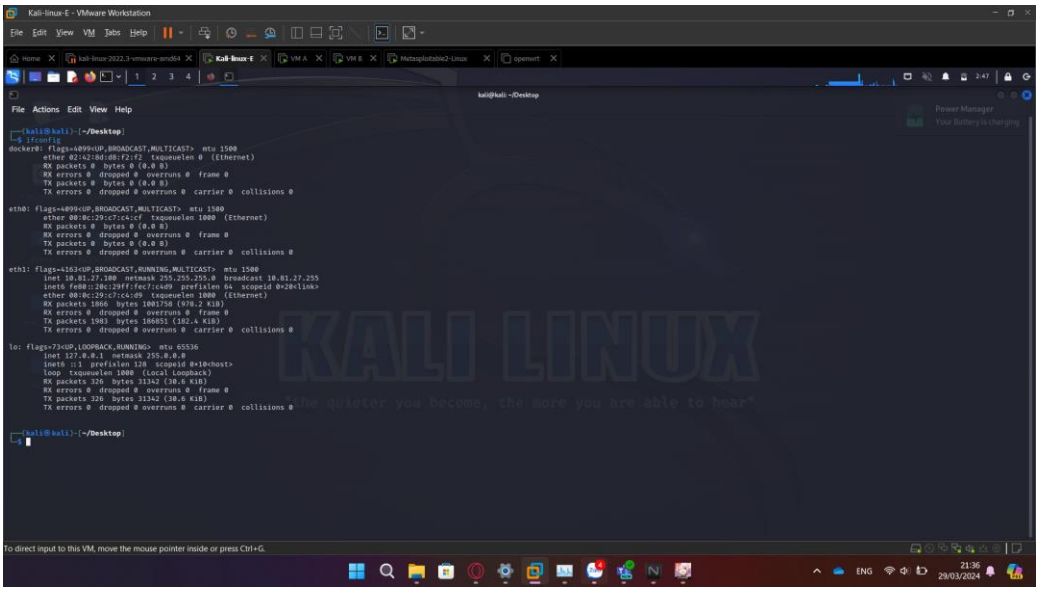
Network Adapter	NAT
Network Adapter 2	Custom (VMnet3)
Network Adapter 3	Custom (VMnet4)

- Gán các card mạng cho máy Victim:

CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet4)
Network Adapter 2	Host-only

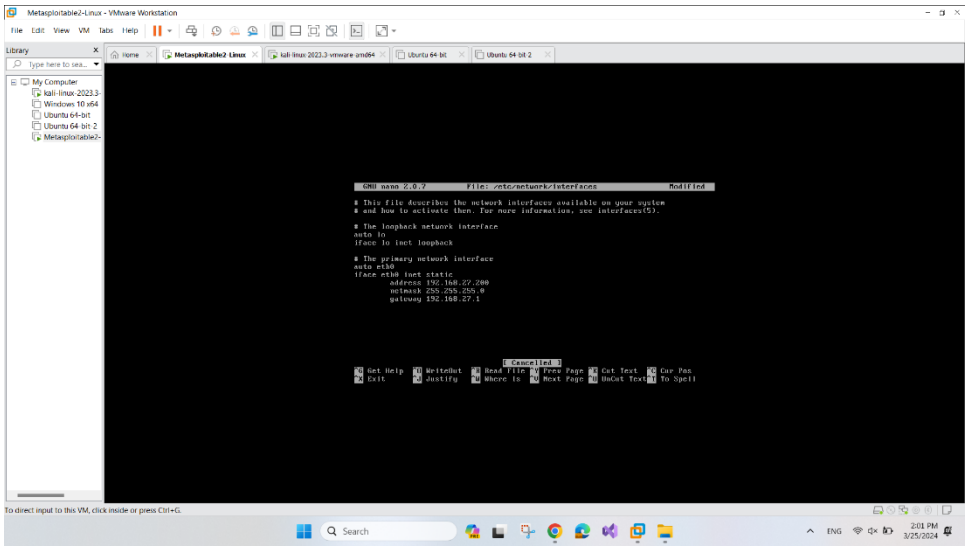
2.1b. Cấu hình địa chỉ IP cho các máy

* Máy Attacker



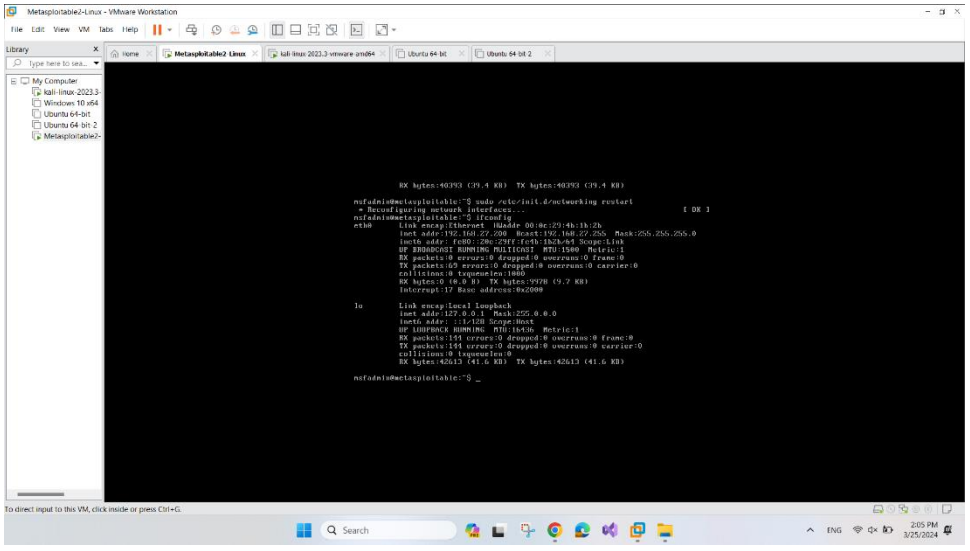
*** Cấu hình địa chỉ IP máy Victim:**

- Nhập lệnh **sudo nano /etc/network/interfaces** và thay đổi nội dung để chỉnh IP:

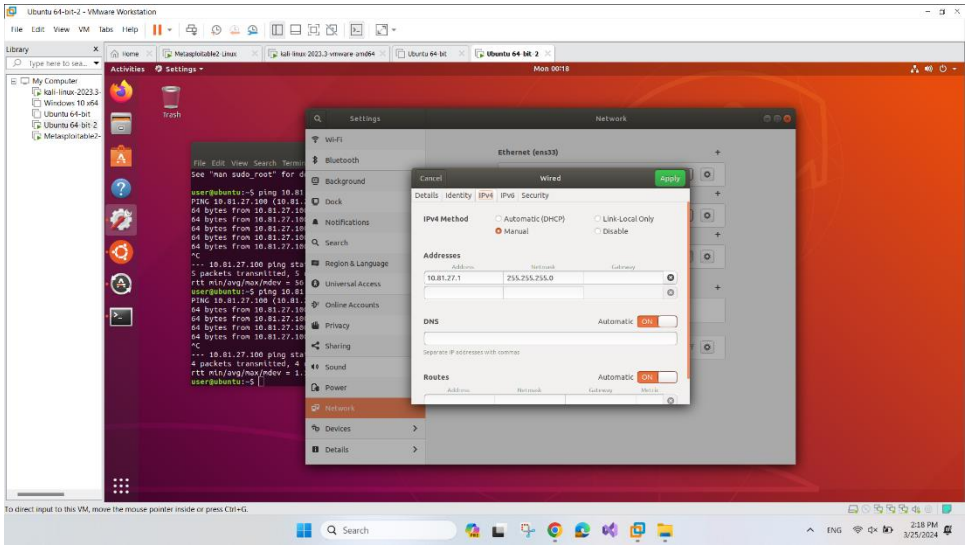


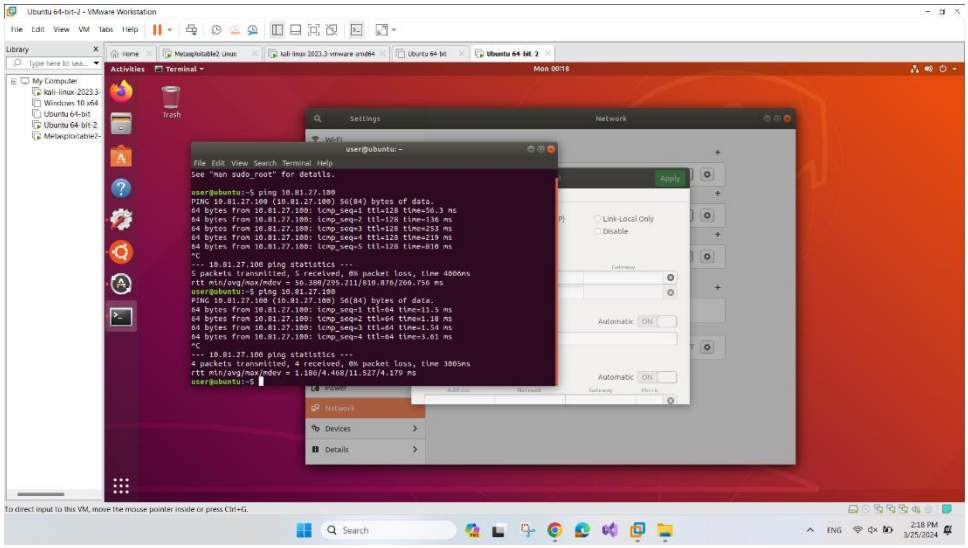
- Restart network: **sudo /etc/init.d/networking restart**

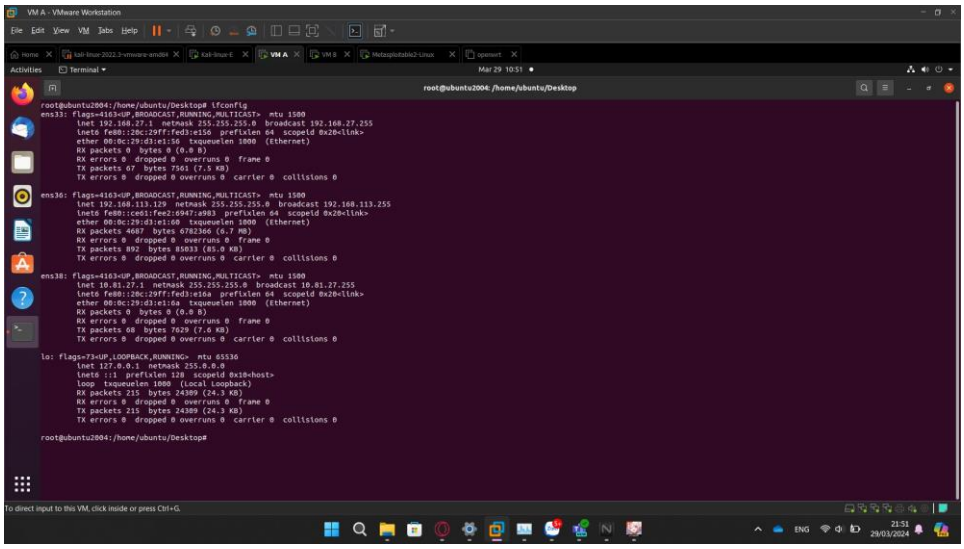
- Kiểm tra IP máy Victim sau khi config



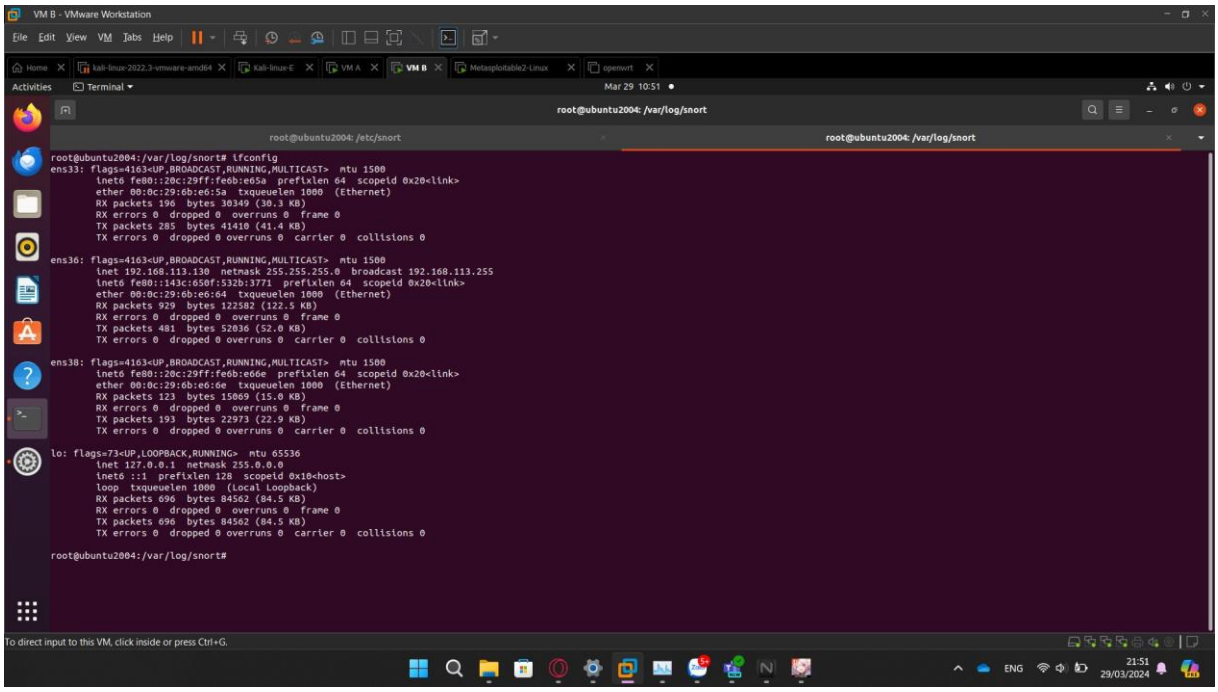
*** Cài đặt IP cho máy Router**





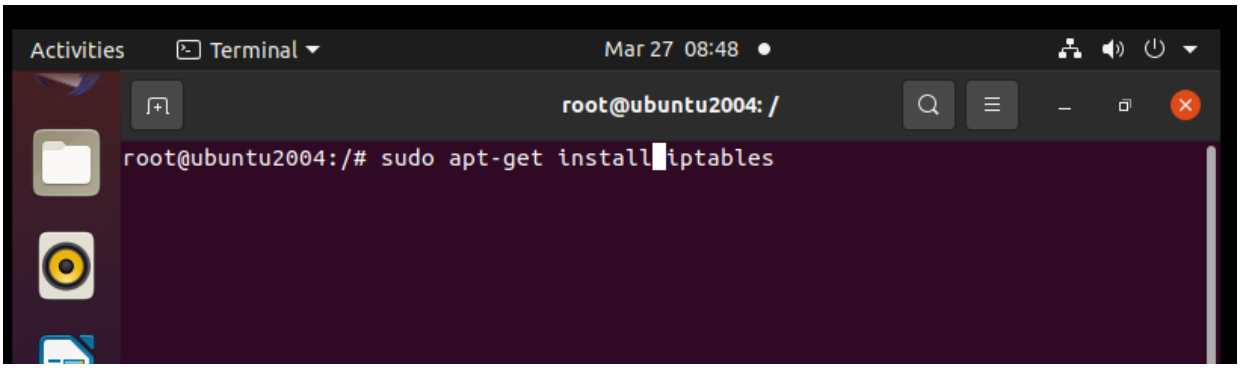


*** Máy Snort:**



2.1c. Cấu hình NAT outbound cho máy router

- Cấu hình NAT outbound cho máy router bằng cách sử dụng công cụ iptables:



- Cấu hình bảng NAT của router bằng các câu lệnh:

iptables -t nat -A POSTROUTING -o ens36 -j MASQUERADE

iptables -A FORWARD -I ens38 -o ens36 state -m --state RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -I ens33 -o ens36 state -m --state RELATED,ESTABLISHED -j ACCEPT

- Cuối cùng là lưu lại cấu hình bằng câu lệnh:

sh -c “iptables-save > /etc/iptables/rules.v4”

*** Kết quả cấu hình bằng iptables và bảng NAT:**

```
root@ubuntu2004:/# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
root@ubuntu2004:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,EST
ABLISHED
ACCEPT     all  --  anywhere             anywhere             state RELATED,EST
ABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu2004:/#
```

- Máy attacker ping google.com:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -w 4 google.com
PING google.com (142.251.220.78) 56(84) bytes of data.
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=1 ttl=127 time=37.2 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=2 ttl=127 time=49.9 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=3 ttl=127 time=37.7 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=4 ttl=127 time=33.7 ms

── google.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 33.656/39.615/49.946/6.162 ms

┌──(kali㉿kali)-[~/Desktop]
└─$
```

- Traceroute ở máy attacker:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ traceroute google.com
traceroute to google.com (142.251.220.46), 30 hops max, 60 byte packets
 1  10.81.27.1 (10.81.27.1)  2.248 ms  1.392 ms  0.940 ms
 2  192.168.30.2 (192.168.30.2)  1.375 ms  1.163 ms  1.081 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

2.1d. Cài đặt và cấu hình Snort

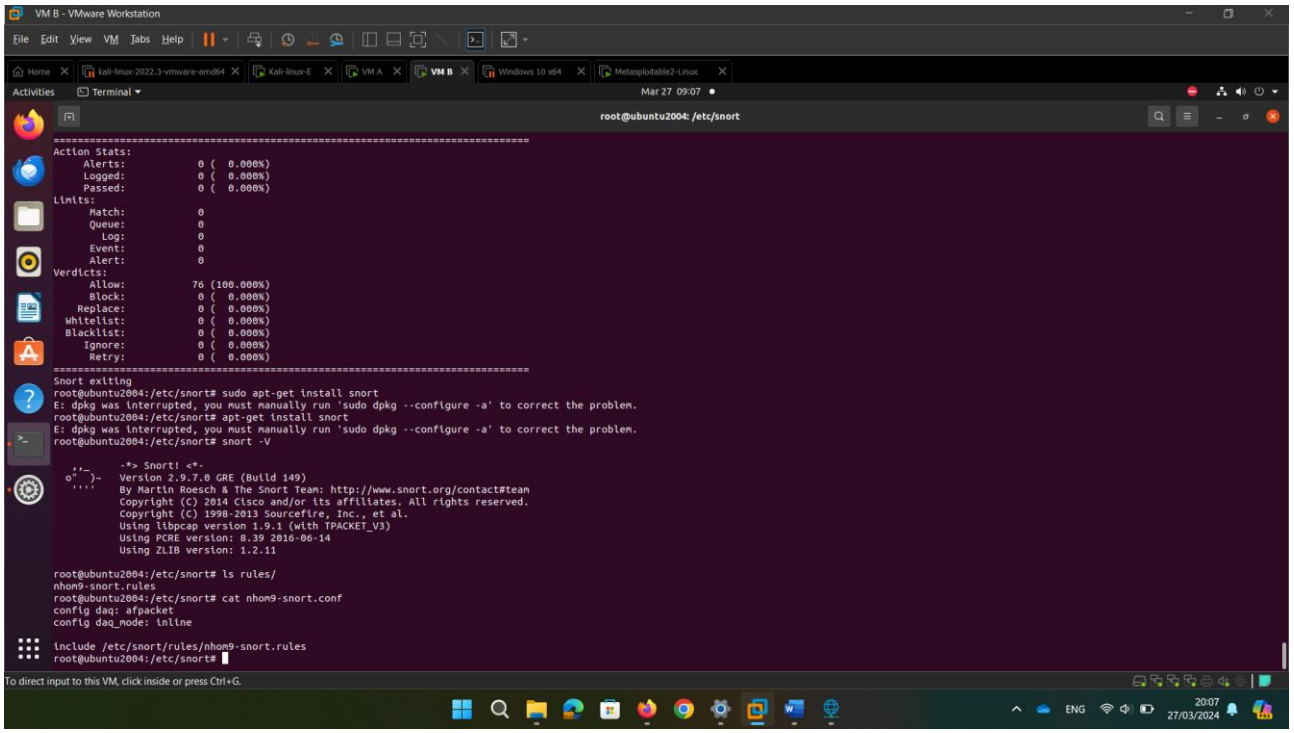
- Cài đặt snort:

```
root@ubuntu2004:/etc/snort# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

root@ubuntu2004:/etc/snort#
```

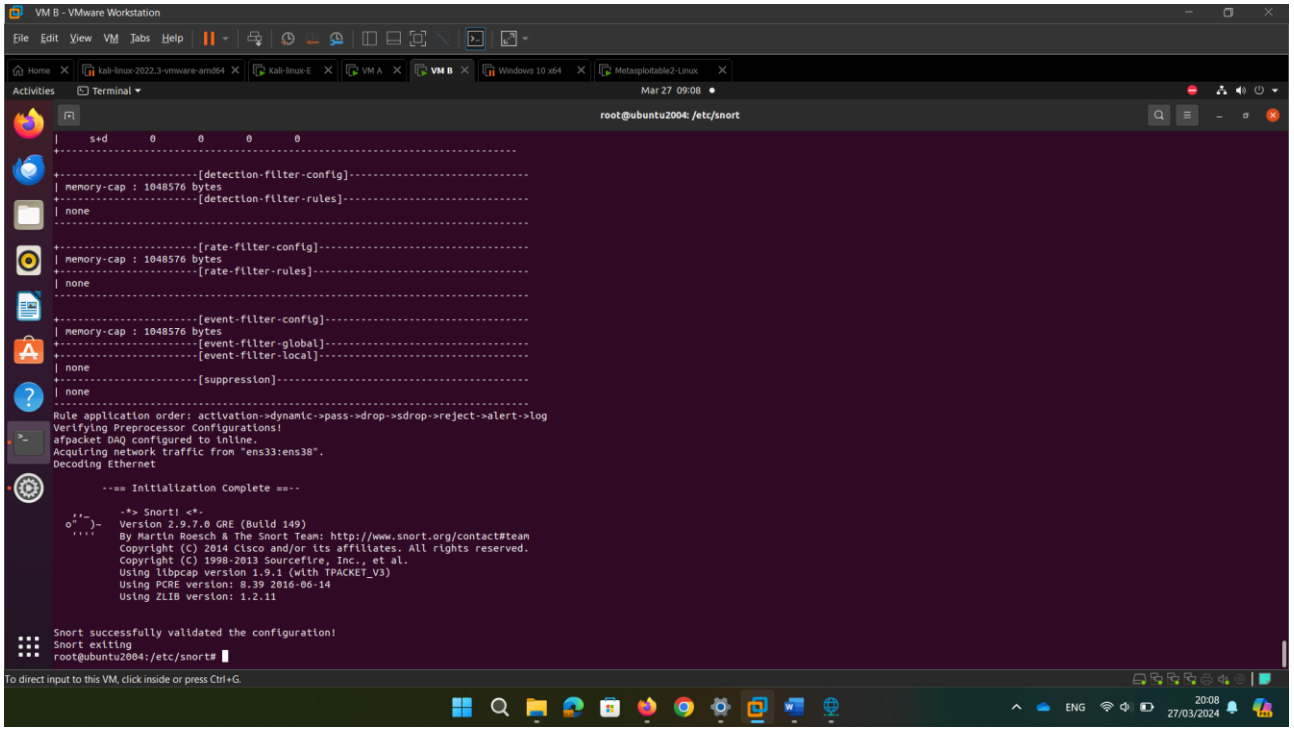
- Tạo file rules riêng cho snort:

```
root@ubuntu2004:/etc/snort# ls rules/
nhom9-snort.rules
root@ubuntu2004:/etc/snort#
```

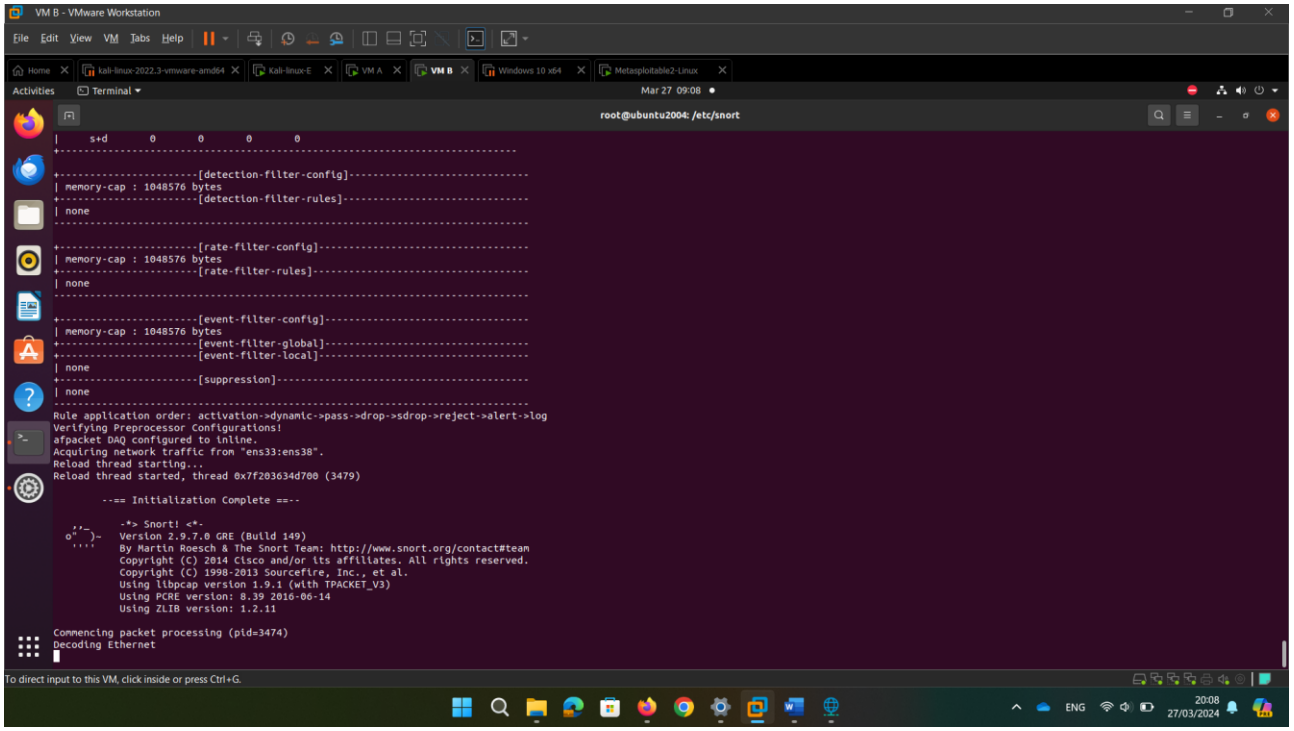
- Tạo và viết file config cho snort:



- Kiểm tra:



- Chạy snort:



- Máy victim ping google.com:

```
msfadmin@metasploitable:~$ ping -w 4 google.com
PING google.com (142.250.66.78) 56(84) bytes of data.
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=1 ttl=127 time
=35.1 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=2 ttl=127 time
=149 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=3 ttl=127 time
=45.0 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=4 ttl=127 time
=41.2 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 35.137/67.828/149.953/47.545 ms
msfadmin@metasploitable:~$
```

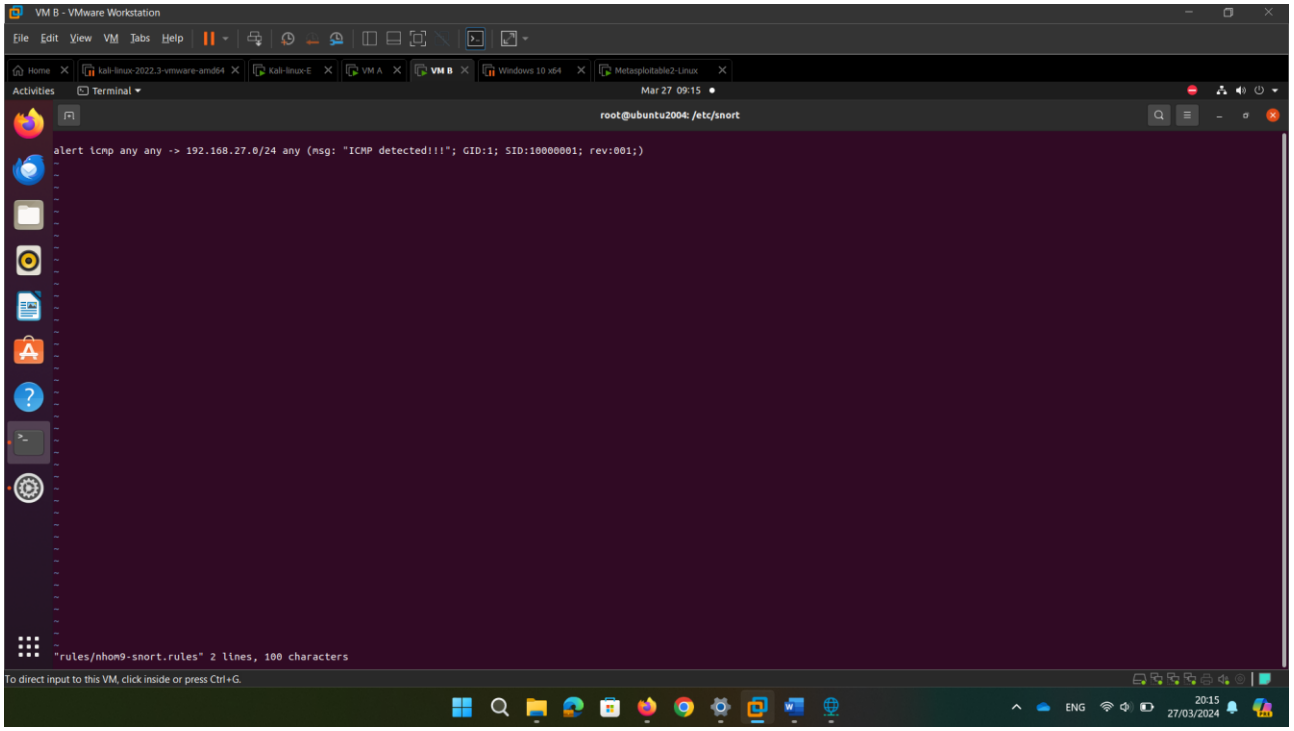
- Máy attacker ping tới máy victim:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -w 4 192.168.27.200
PING 192.168.27.200 (192.168.27.200) 56(84) bytes of data.
64 bytes from 192.168.27.200: icmp_seq=1 ttl=63 time=2.39 ms
64 bytes from 192.168.27.200: icmp_seq=2 ttl=63 time=7.24 ms
64 bytes from 192.168.27.200: icmp_seq=3 ttl=63 time=2.12 ms
64 bytes from 192.168.27.200: icmp_seq=4 ttl=63 time=28.7 ms

── 192.168.27.200 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.116/10.107/28.690/10.920 ms
```

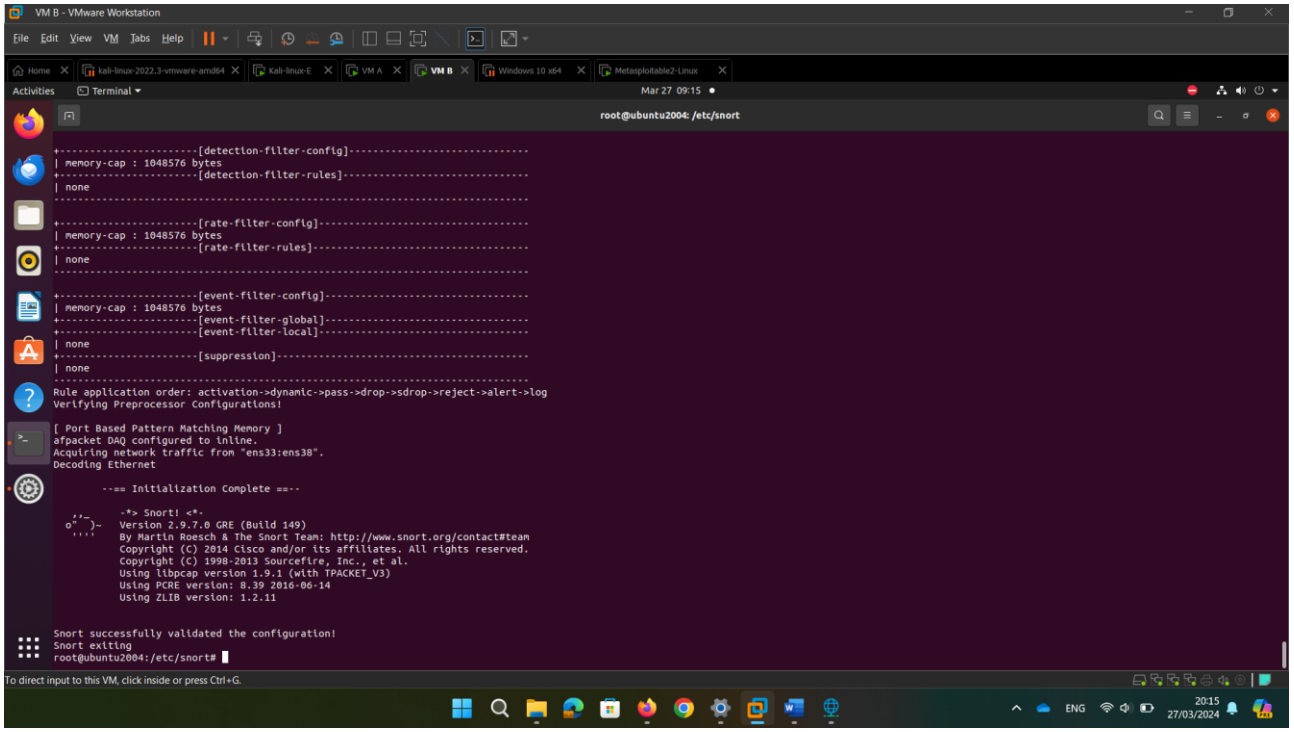
2.1e. Viết rule cho Snort

- Viết Rules:

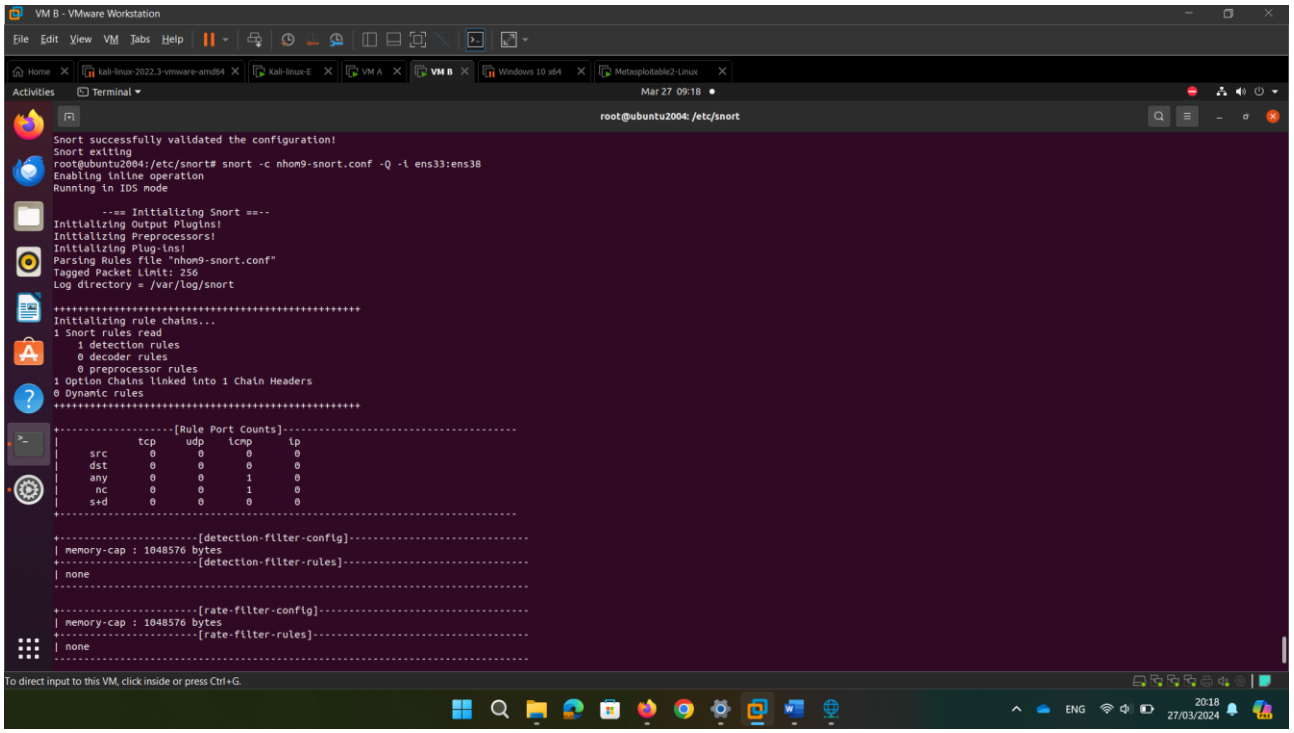
alert icmp any any -> 192.168.27.0/24 any (msg: "ICMP detected!!!"; GID:1; sid:10000001; rev:001;)



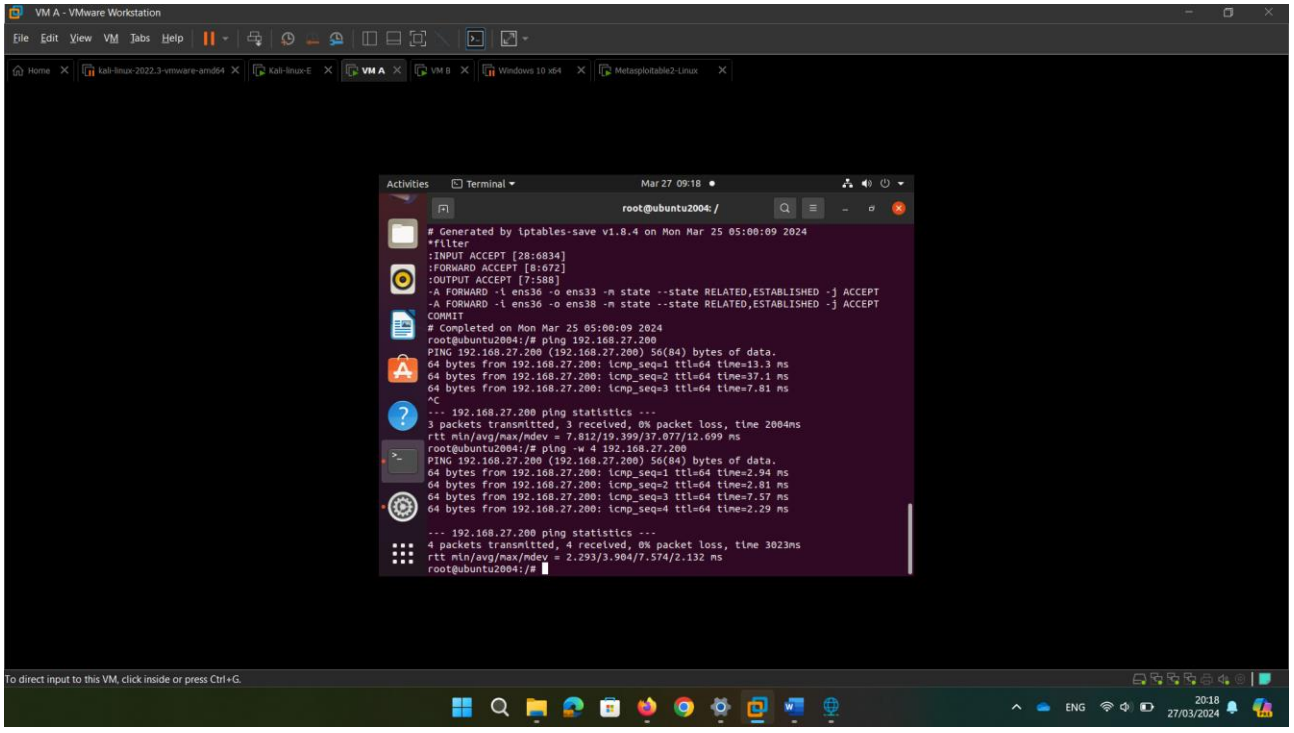
- Kiểm tra:



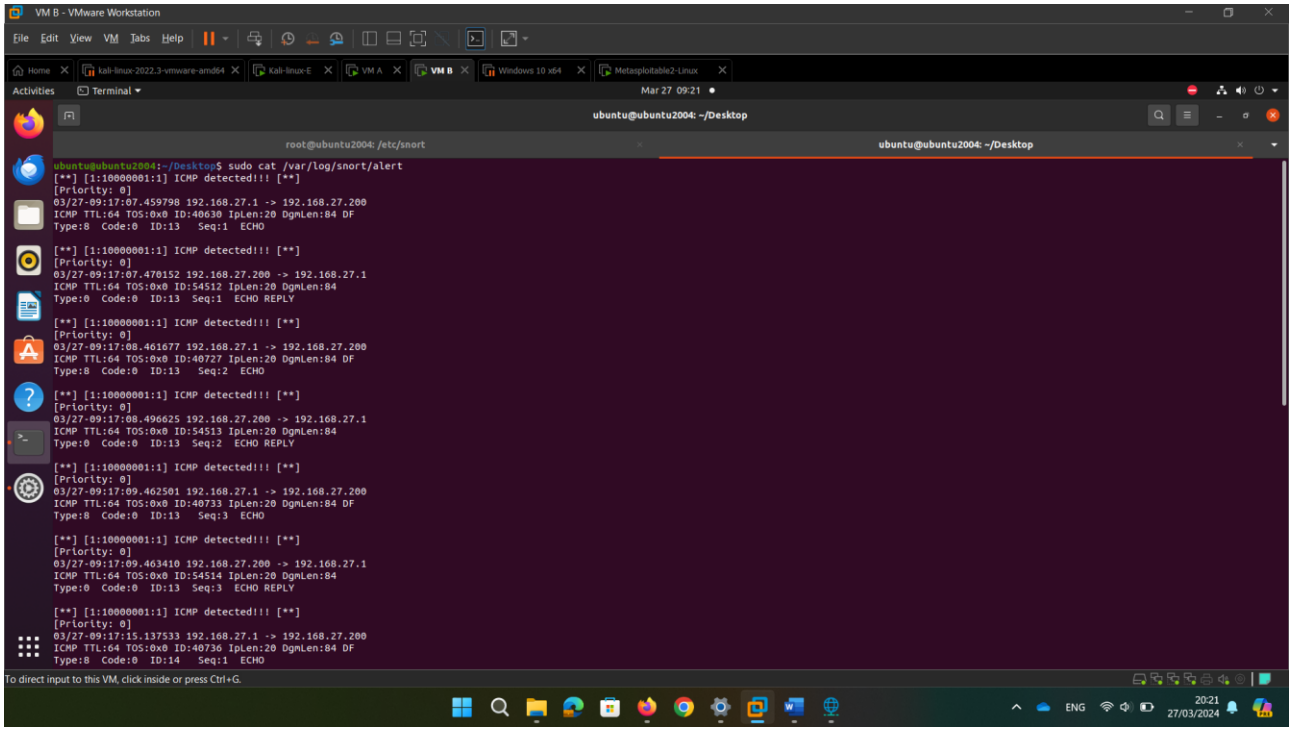
- Chạy snort và kiểm tra ping từ máy router đến victim:



+ Máy router ping:



+ Kiểm tra log:



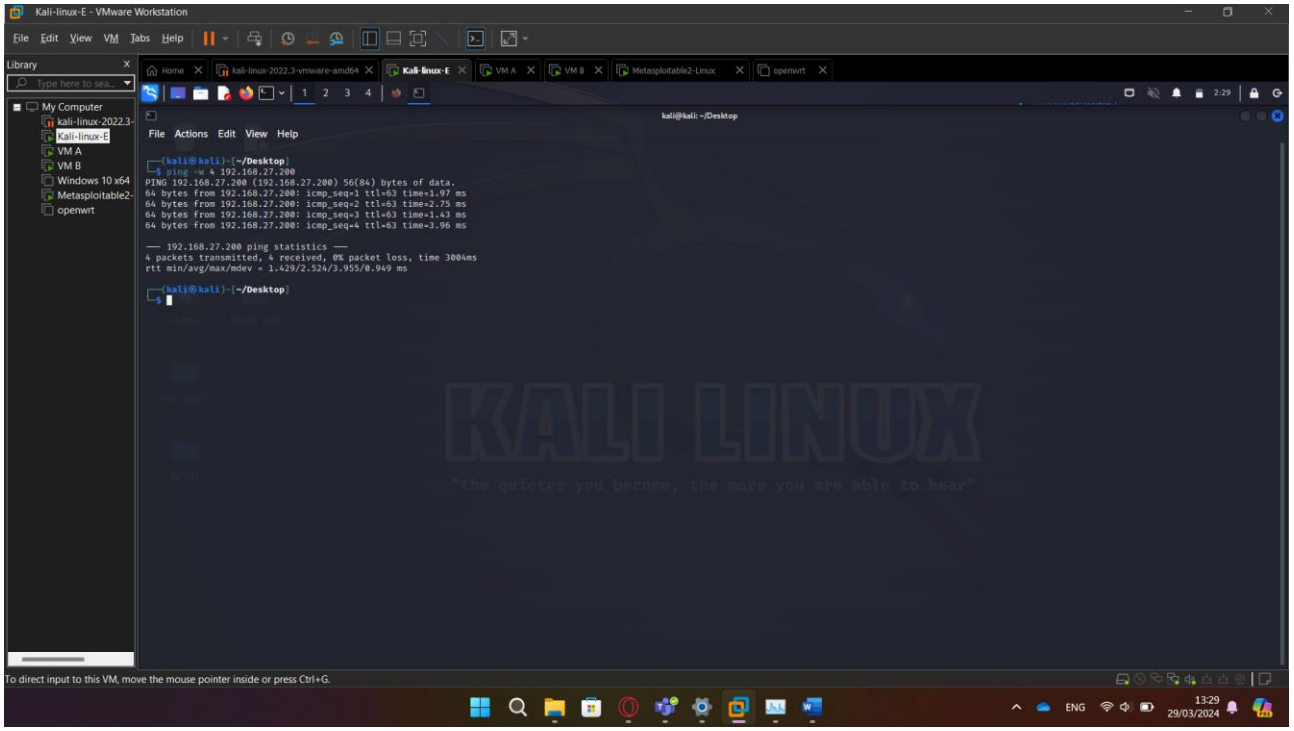
3. Yêu cầu 3: Sinh viên viết rule drop các gói ICMP đi đến máy Victim (rule #1). Sử dụng tcpdump trên máy Victim

* **Rules:** drop icmp any any -> 192.168.27.0/24 any (msg: “ICMP test dropped”; sid:1000001; rev:001;)

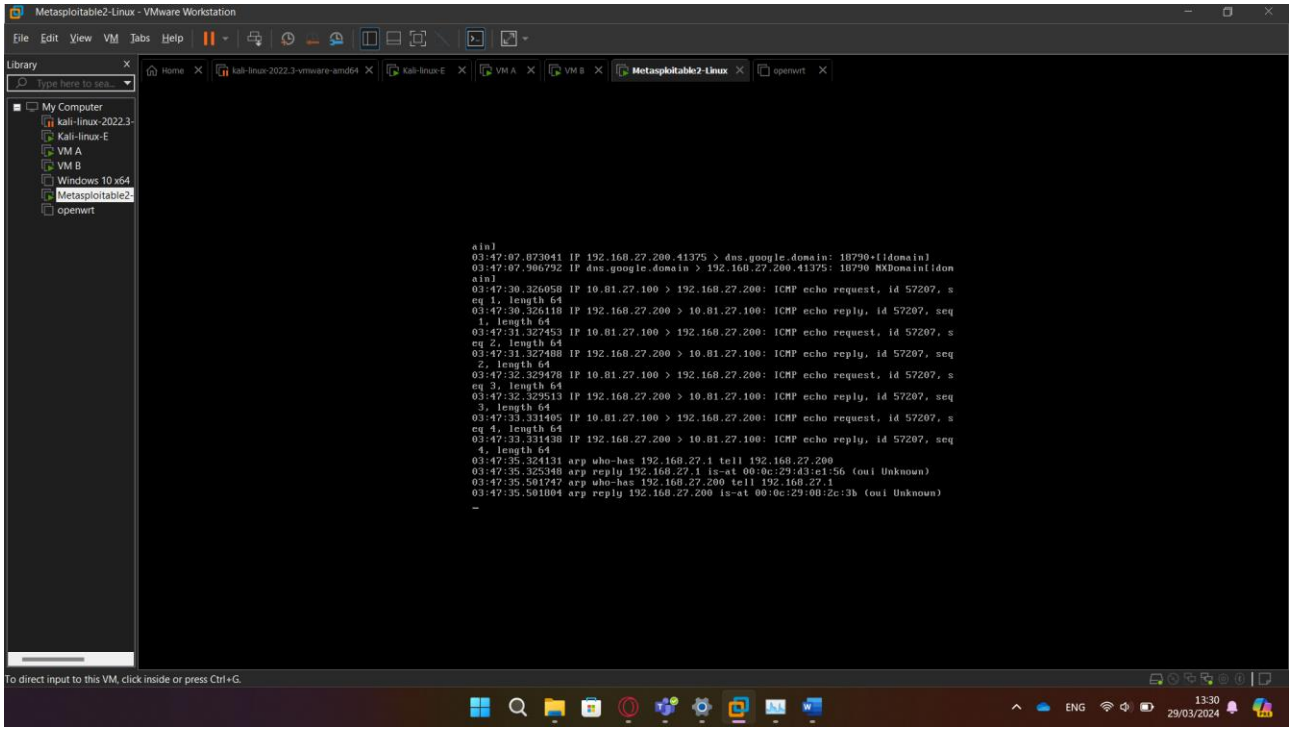
*** Kiểm tra alert log của Snort để xem kết quả**

- Trước khi viết áp dụng rule #1.

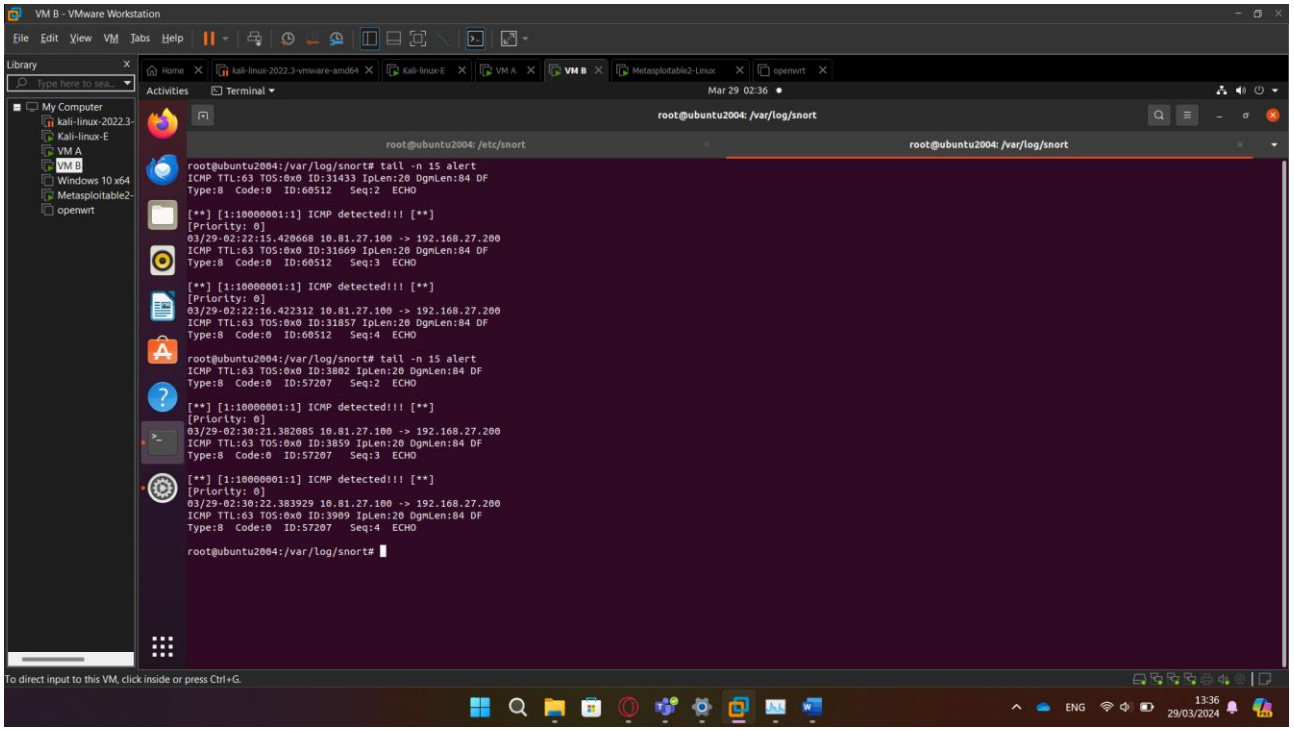
+ Máy attacker ping đến victim:



+ Tcpdump trên máy victim:

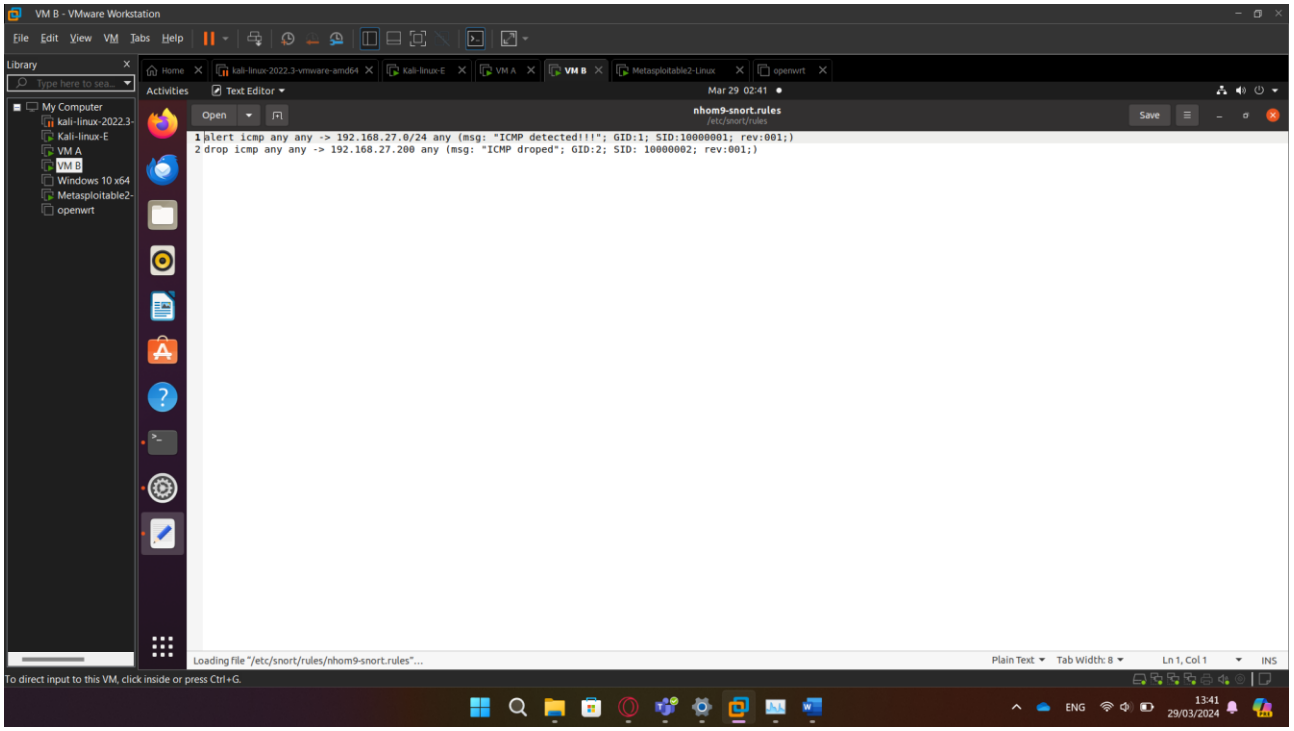


+ Alert log của snort:

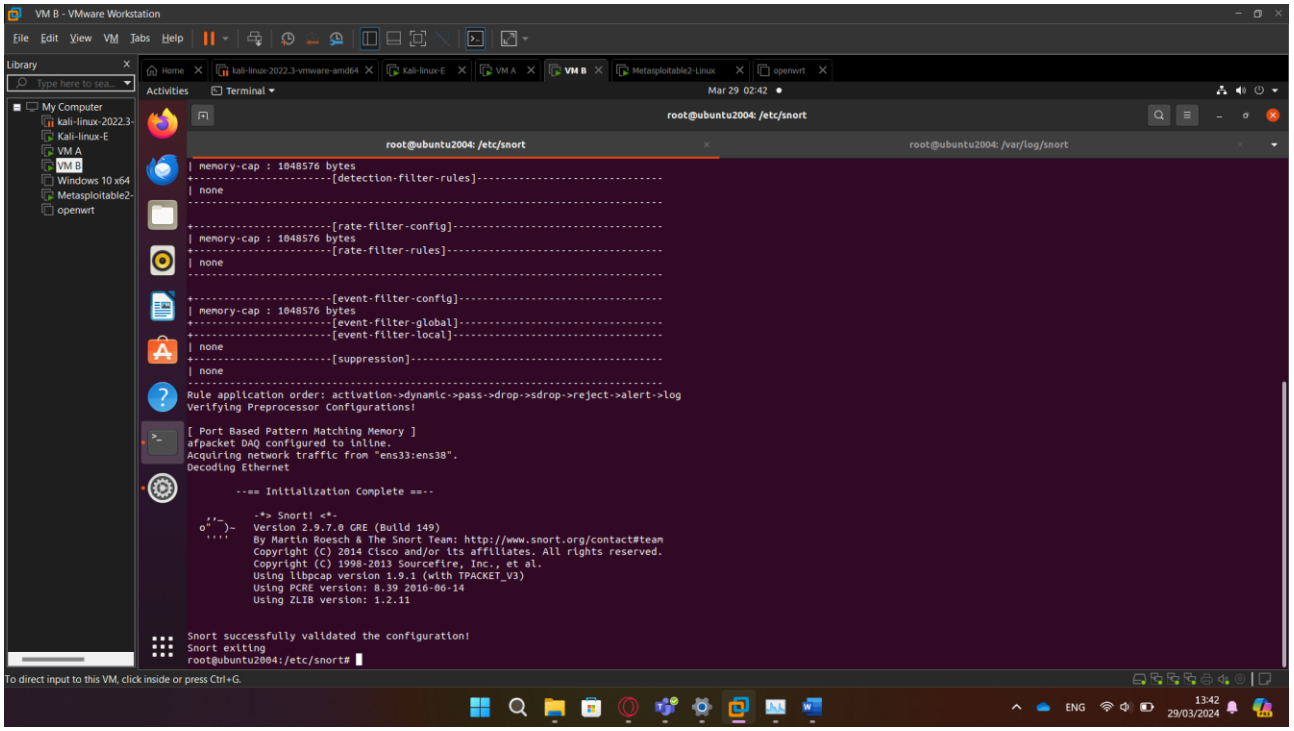


- Sau khi áp dụng rule #1.

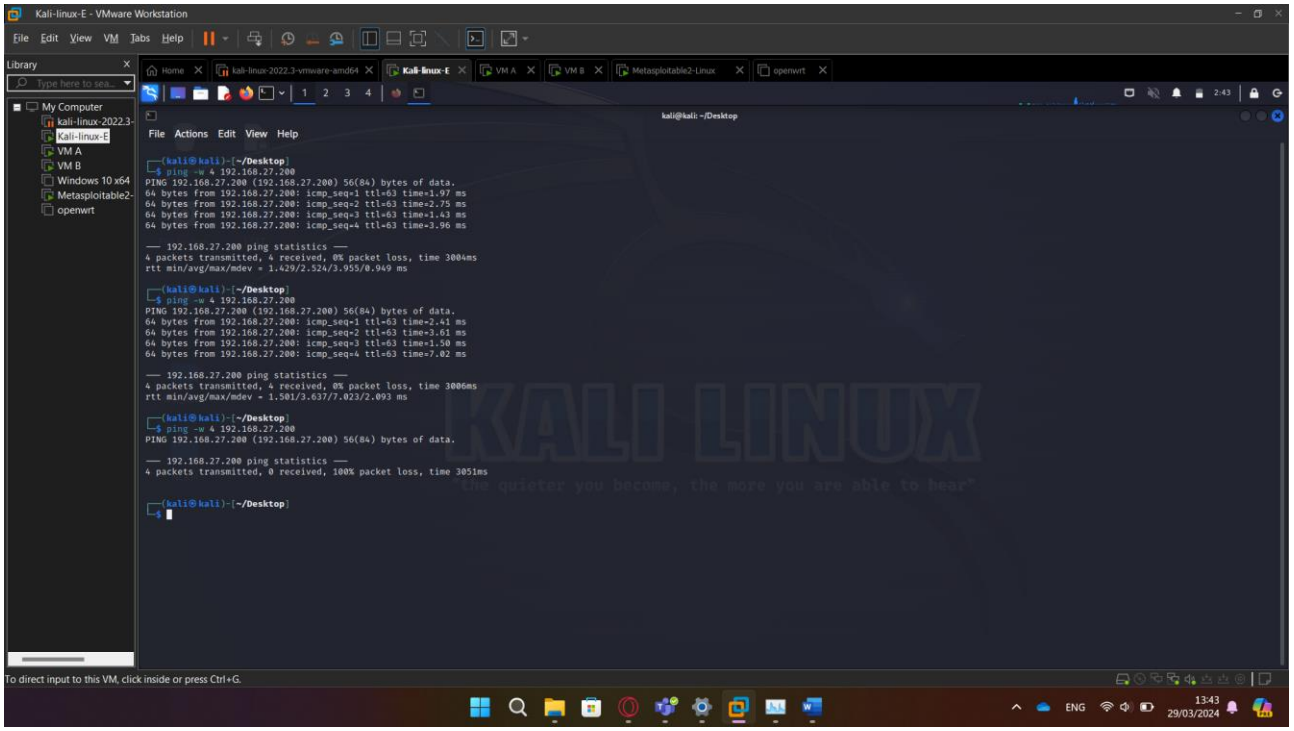
+ Thêm rule mới vào file rules:



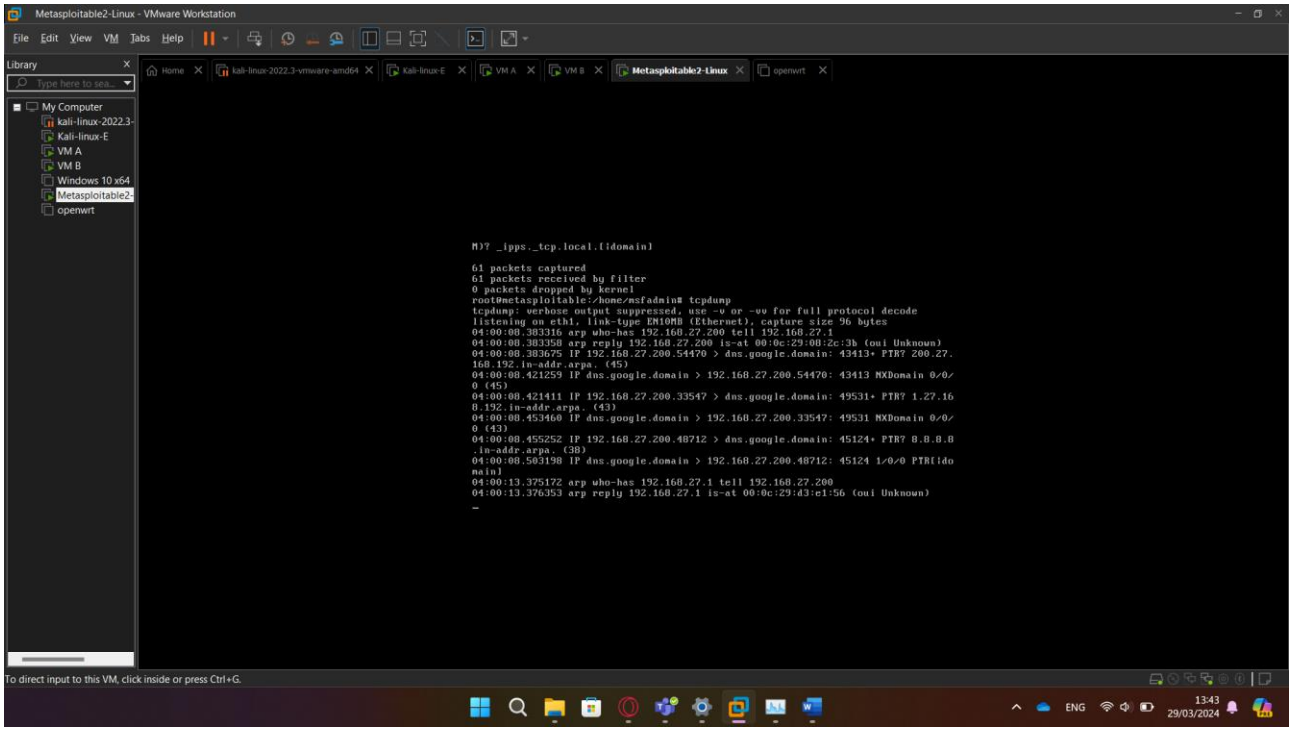
+ Kiểm tra rule:



+ Máy attacker ping đến victim:



+ Tcpdump ở máy Victim:



+ Alert log của snort, lúc này snort sẽ có 2 file alert: 1 file chứa thông báo drop (file alert), file còn lại chứa thông báo của alert (file alert.1):